Virtual Private Networks, 2nd Edition
By Mike Erwin, Charlie Scott, Paul Wolfe

Table of Contents

Chapter 4. Implementing Layer 2 Connections

4.2 How PPTP Works

As a tunneling protocol, PPTP encapsulates network protocol datagrams within an IP envelope. After the packet is encapsulated, any router or machine that encounters it from that point on will treat it as an IP packet. The benefit of IP encapsulation is that it allows many different protocols to be routed across an IP-only medium, such as the Internet.

The first thing to understand about PPTP is that it revolves around Microsoft RAS for Windows NT. RAS allows a network administrator to set up a Windows NT server with a modem bank as a dial-in point for remote users. Authentication for the RAS users takes place on the NT server, and a network session is set up using the PPP protocol. Through the PPP connection, all of the protocols allowed by RAS can be transported: TCP/IP, NetBEUI, and IPX/SPX. To the RAS users it appears as though they're directly connected to the corporate LAN; they notice no difference between RAS through direct dial-in and RAS over the Internet.

PPTP was designed to allow users to connect to a RAS server from any point on the Internet and still have the same authentication, encryption, and corporate LAN access they'd have from dialing directly into it. Instead of dialing into a modem connected to the RAS server, the end users dial into their ISPs and use PPTP to set up a "call" to the server over the Internet. PPTP and RAS use authentication and encryption methods to create a virtual private network.

There are two common scenarios for this type of VPN: in the first, a remote user is dialing into an ISP with a PPTP-enabled remote access switch that connects to the RAS server; in the second, the user is connecting to an ISP that doesn't offer PPTP, and must initiate the PPTP connection on their client machine.

4.2.1 Dialing into an ISP That Supports PPTP

Dialing into an ISP that supports PPTP requires three things:

- The network with which you want to establish a VPN must have a PPTP- enabled Window NT 4.0 RAS server. By "PPTP-enabled" we mean that the PPTP protocol is installed and there are VPN dial-up ports set up in RAS. The server must also be accessible from the Internet.

- Your ISP must use a remote access switch that supports PPTP, such as the Ascend MAX 4000 series or a U.S. Robotics Total Control Enterprise Network Hub. (Together, these two products make up a significant portion of the ISP dial-up hardware market.)

- Your ISP has to actually offer the PPTP service to users, and must enable it for your

account.

To offer a typical scenario, a central corporate office in Denver has set up a Windows NT 4.0 server running PPTP and RAS. A sales manager named Sara N. is at a conference in Atlanta, and wants to dial into the corporate network to check her email and copy a presentation from her desktop machine. Her remote system is a Windows 95 laptop computer with a 28.8Kbps modem. She's obviously out of the local dialing area of her office, but has an account through a national ISP that supports PPTP through their U.S. Robotics remote access switches. The ISP was told the IP address of the RAS server at Sara N.'s corporate office, and has added it to her user profile. The IP address is 2.1.1.60.

When the sales manager dials into her PPTP-enabled ISP, the following events occur:

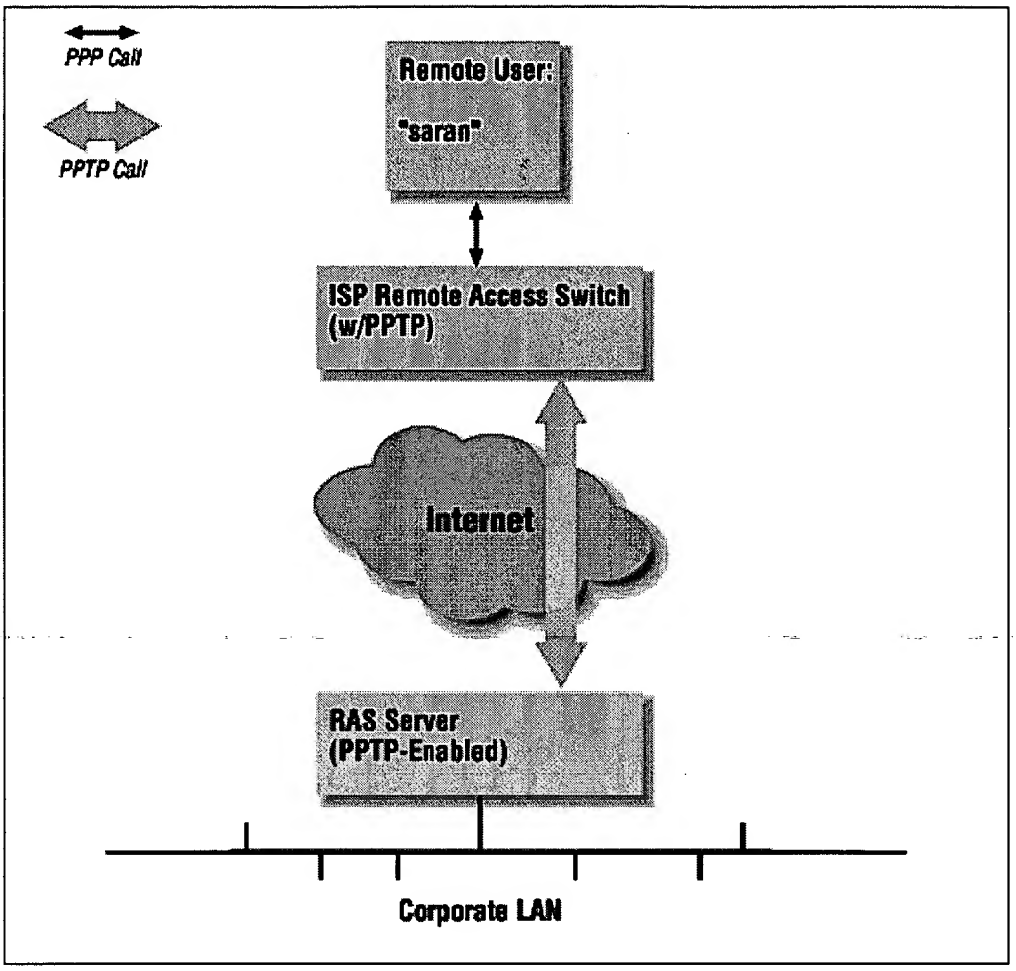
1. Sara N. initiates a call into her ISP's POP using Microsoft's Dial-Up Networking. She logs in with her username, "saran." Doing so starts a PPTP session between the ISP's remote access switch and the corporate office's NT server, whose IP address is specified in Sara N.'s user profile as 2.1.1.60.

2. Sara N.'s PPP session is tunneled through the PPTP stream, and the NT RAS server authenticates her username and password and starts her PPP session. Essentially, this all takes place just as if she were dialing into the RAS server via a directly connected modem.

3. The PPTP session can then tunnel the protocols that dial-up users are allowed to use. In Sara N.'s case, TCP/IP is one of those protocols, and the NT RAS server assigns her machine the internal corporate IP address of 2.1.1.129.

Looking at Figure 4-1, you can follow these events and see where the client's original Point-to-Point Protocol (PPP) session is encapsulated by the PPTP tunnel. This figure is a simplified version of what the actual topology looks like—routers at the ISP and corporate LAN, for instance, have been removed.

Figure 4-1. Dialing into an ISP that supports PPTP



Once the PPTP is completed and the sales manager is authenticated, she has access to the corporate network as if she were on the LAN. She can then check her email and access files on her desktop machine using file sharing.